REMARKS

Status:

Claims 1-3 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. And, claims 1-12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the teaching of U. S. Pat. No. 5,923,756 to Shambroom, considered with the teaching of Schneier in "Applied Cryptography" in view of the teaching of Balenson, " Privacy Enhancement for Internet Electronic Mail: Algorithms, Modes, and Identifiers", Network Working Group, Request For Comments (RFC) 1423, February 1993.

Claims 1-12 as amended are presented for reconsideration as explained in the analysis that follows.

Analysis:

Claim 1 has been amended to clarify the subject matter of claims 1-3 as being structure for functioning in a computer apparatus which reads and interprets the stored certificate to control cryptographic operations.. It is believed this satisfies 35 U.S.C. §101 and a withdrawal of the rejection based thereon is respectfully solicited. Applicant would welcome suggestions if further refinement is needed

As regards X.509 Certificates, (see "Standard" at Attachment A of Applicant's previous amendment or http://www.ietf.org/rfc/rfc2459.txt) the Standard spells out in detail the profile to be followed. Section 4.1 of the Standard specifies the content of the basic certificate fields. At Section 4.1.2.7 there is provision for only one public key and one algorithm associated with that key.. Section 4.2 then describes the extensions. . The Standard proposes uses of extensions but does not mention using them to identify alternative cryptographic algorithms and corresponding public keys. Indeed it specifies one algorithm in the certificate body and makes no suggestion for inclusion of cryptographic algorithms in an extension.

Serial No. 09/240,265   6   Docket CR9-98-095

Applicant provides a clever way to transfer alternatives with respective public keys while not violating the ITU X509 Standard. Applicant uses certificate extensions in an way not taught or suggested in the version 3 Standard. This allows a compliant certificate to support one or more alternative cryptographic algorithms so that a selection other than that of the base certificate does not require resort to a new certification hierarchy.

Now considering the Schneier reference at Figure 24.2, it appears to describe no more than the original X509 standard, that is, the base certificate without extensions (see Standard at Section 4.1.1 which describes required fields). Applicant disagrees with the Office Action at p. 4, section 6 which states Schneier Figure 24.2 shows "certificate extensions". Which box shows a certificate extension? They all appear to show base certificate required fields.
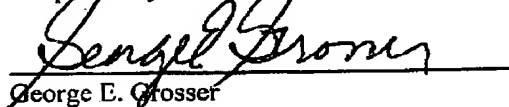
Shambroom (see col10, lines. 30-38), provides lists of algorithms but mentions one public key. Furthermore, Shambroom does not teach or suggest using extensions to transfer a public key for an alternative cryptographic algorithm (see applicant's claim 1, lines 7-10). Only an algorithm list is taught. With this approach the alternatives are not supported and a change of algorithm involves a new certificate hierarchy. Re-certifying is the prior art solution for making a new choice. Shambroom teaches nothing more.

Balenson explains the need for improved cryptographic algorithms; but, fails to teach or suggest Applicants delivery approach using certificate extensions. At section 4.3, cited at page 5 of the Office Action, Balenson does not mention extensions, much less, extensions that identify alternatives to the base certificate algorithm, and respective public keys. It seems, at section 4.3, that Balenson is describing various "alternatives" for the base certificate and intends that only one choice be made. Again it seems a change of algorithm involves a new certificate hierarchy. Where is the teaching of a usable alternative to the base certificate algorithm carried in extensions to the certificate itself, as opposed to, proposed alternatives for the single base certificate algorithm. This is a chasm too wide to bridge with the skill of the art.

Serial No. 09/240,265   7   Docket CR9-98-095

Note, again, that Applicant's certificate has the usual first algorithm and public key but also offers usable algorithm choices in extensions, algorithm choices paired with respective public keys to be usable without requiring a new certificate hierarchy. This allows a certificate for a popular, less secure algorithm to support, for example, a higher security algorithm as an alternative - not merely suggest it for a new certificate. This advantageous approach is not believed to be taught or even suggested in the prior art.

In accordance with the foregoing, it is believed that the subject Application clearly identifies inventive subject matter not taught or suggested in the prior art. Hence Applicant respectfully solicits withdrawal of the rejection of claims under 35 U.S.C. §103(a) and early notice that this case has been placed in condition for allowance.

Respectfully Submitted,

George E. Grosser

Reg. No. 25,6291

c/o IBM Corp.
Dept. T81/Bldg. 503 PO Box 12195
Research Triangle Park, NC 27709
(919)968-7847   Fax 919-254-4330
EMAIL: gegch@prodigy.net

Serial No. 09/240,265   8   Docket CR9-98-095